UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

REY BORGE, individually and on behalf of all others similarly situated, Plaintiff, v. MR. COOPER GROUP INC., Defendant.	)	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Rey Borge ("Plaintiff"), by his undersigned counsel, files this Class Action Complaint, individually and on behalf of a class of all similarly situated persons, against Defendant Mr. Cooper Group Inc. ("Defendant" or "Mr. Cooper"). Plaintiff bases the following allegations upon personal knowledge as to his own acts and otherwise on information and belief and the investigation of counsel, and states the following:

INTRODUCTION

1. Plaintiff brings this class action on behalf of himself and all other individuals ("Class Members") whose sensitive personal information was disclosed to unauthorized third parties during a massive data breach that was purportedly discovered by Defendant on October 31, 2023 (the "Data Breach").

2. Upon information and belief, personally identifiable information ("PII") was compromised in the Data Breach, including important information related to home loans such as Plaintiff's and the Class Members' names, dates of birth, addresses, and social security numbers, and potentially other similarly sensitive information including banking information.

3. As Defendant is or should have been aware, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. For example, fraudsters attempt to utilize financial information to make fraudulent transactions and purchases, or use a collection of personal data to take out fraudulent loans. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to the Class Members.

4. Defendant Mr. Cooper Group Inc. operates the brand Mr. Cooper, which is the third largest home loan servicer in the United States.[1] Defendant serves 4.3 million customers nationwide, including at least 3.8 million homeowners.[2] Defendant's servicing portfolio includes $937 billion in unpaid principal balance.[3] Many of the mortgage loans held by Mr. Cooper did not originate there, but instead originated with other mortgagers and were later sold or transferred to Mr. Cooper. Consequently, Mr. Cooper has sensitive information on millions of individuals who had no say in Mr. Cooper obtaining or servicing their loans, nor any ability to prevent their sensitive information from falling into Mr. Cooper's hands.

5. Prior to and through October 31, 2013, Defendant obtained the PII of Plaintiff and the Class Members.

6. Defendant touts that it is technologically competent and that it is capable of and committed to protecting and maintaining its customer's sensitive information.[4]

7. In reality, Defendant's pronouncements as being capable a data custodian proved false. Contrary to its many representations and promises, Defendant utilized inadequate data

[1] https://www.mrcoopergroup.com/.
[2] https://www.mrcooper.com/about-us/overview; https://www.mrcooper.com/about-us/purpose.
[3] https://www.mrcoopergroup.com/.
[4] *See* https://www.mrcooper.com/privacy.

security measures it knew, or should have known, put the highly sensitive data it oversaw at significant risk of theft by or exposure to nefarious parties.

8. On or before October 31, 2023, these risks came to fruition, and Defendant experienced a significant data breach on its systems.

9. On or around November 2, 2023, Defendant began notifying Plaintiff and Class Members of the Data Breach. The notifications sent to Plaintiff and the Class do not include any, let alone sufficient, identification of the PII that was exposed to allow Plaintiff and the Class to take all steps necessary to mitigate the harms. Further, Defendant failed to inform Plaintiff and the Class Members of the specific vulnerabilities and root causes of the Data Breach.

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and the Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

11. The exposed PII of Plaintiff and the Class Members can be sold on the dark web. Hackers can access and then offer for sale the PII to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft and the sharing and detrimental use of their sensitive information.

12. The PII was compromised due to Defendant's negligent and careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members.

13. Plaintiff Rey Borge one of millions of victims of the Data Breach. He is a resident of California whose PII was compromised by the Data Breach.

14. Plaintiff and the Class Members remain at a continued risk of harm due to the exposure and potential misuse of their sensitive personal information by criminal hackers. In fact, the full scope of the harm caused by the data breach is yet unknown, and as of this date Defendant

has failed to inform Plaintiff and the Class Members exactly which and how much of their PII was exposed. As discussed below, in fact, Defendant has provided contradictory information as to what information was stolen, including whether it includes banking information.

15. As such, Plaintiff brings this Complaint on behalf of persons whose PII was stolen during the Data Breach. Plaintiff asserts claims for negligence, negligence per se, and for declaratory and injunctive relief.

JURISDICTION

16. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, diversity is satisfied because at least one Class Member is a citizen of a different state than Defendant. Further, Plaintiff alleges that in the aggregate the claims of all purported class members exceed $5,000,000, exclusive of interest and costs.

17. This Court has general personal jurisdiction over Defendant Mr. Cooper Group Inc. because Defendant is headquartered in Coppell, Texas. Defendant has sufficient minimum contacts with Texas because it conducts substantial business in the state.

18. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred within the Dallas Division of the Northern District of Texas and because Defendant conducts a substantial part of its business within the Dallas Division of the Northern District of Texas.

PARTIES

19. **Plaintiff** Rey Borge is a citizen of California who was the authorized payor on a home loan serviced by Defendant Mr. Cooper. Subsequent to and because of the Data Breach, Borge experienced effects of his information being compromised and used nefariously, including marked increase in suspicious text messages, call, and emails.

20. **Defendant** Mr. Cooper Group Inc. is a for-profit Delaware corporation with its principal place of business at 8950 Cypress Waters Boulevard, Coppell, Texas 75019.

FACTS

A. Defendant Provides Services Involving Highly Sensitive Data

21. Defendant is a company headquartered in Coppell, Texas that provides home loan services to individuals across the United States.

22. To provide these services, Defendant collects, obtains, maintains, and handles the sensitive personal information of millions of individuals, including social security numbers, names, dates of birth, addresses, and banking information.

23. Defendant acknowledges how critical it is to safeguard this information—and, likewise, how devastating it is to individuals whose information has been stolen. Defendant proclaims that "[k]eeping financial information is on of our most important responsibilities"; that "[o]nly those persons who need it to perform their job responsibilities are authorized to access your information;" that it will "protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards"[5]; and that it will "protect your personal

[5] https://www.mrcooper.com/privacy.

information from unauthorized access and use" through "security measures that comply with federal law … include[ing] computer safeguards and secured files and buildings."[6]

24. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Despite Defendant's promises to protect sensitive data and efforts to portray itself as a capable data custodian, Defendant's own data security decisions created substantial gaps that Defendant knew or should have known created a risk of a data breach. That risk materialized in October 2023, when hackers broke into Defendant's systems and stole highly sensitive data at will and put Plaintiff and the Class at risk that their data would be misused and cause them harm.

B. Defendant Exposed Highly Sensitive Data to Hackers

26. On or about November 2, 2023, Defendant emailed Plaintiff and Class Members a "Notice of Cyber Security Incident" to inform them of the data breach. In its entirely, the Notice reads as follows:

> On October 31, Mr. Cooper became the target of a cyber security incident and took immediate steps to lock down our systems in order to keep your data safe. We are working to resolve the issue as quickly as possible.
> Rest assured, you will not incur and fees, penalties or negative credit reporting related to late payments as we work to fix this issue.
> For updated information, we encourage you to visit https://incident.mrcooperinfo.com/.
> We value you as our customer and are truly sorry for any inconvenience or concern this incident may have caused.

---

6 https://www.mrcooper.com/reference_documents/apollo_mr_cooper/MrCooper_Privacy_Notice.pdf.

27. The website maintained by Defendant to inform its customers of updates regarding the Data Breach (the "Incident Website") contains little more information than the emailed notice, and what information it does contain has been contradictory over time.

28. For example, as of November 9, 2023, the Incident Website stated that "Mr. Cooper does not store banking information related to mortgage payments on our systems. This information is hosted with a third-party provider and, based on the information we have to date, we do not believe it was affected by this incident. As a result, we do not believe that any of our customers' banking information related to mortgage payments was impacted."[7]

29. Defendant no longer stands by those statements. As of November 13, 2023, the Incident Website no longer claims that banking information related to mortgage payments is not stored on Defendant's servers, and no longer states that Defendant believes that customers' banking information was not impacted.[8] On this basis, upon information and belief, banking information related to mortgage payments was among the PII that was stored on Defendant's servers and/or was exposed in the Data Breach.

C. Defendant's Insufficient Data Security Caused the Data Breach

30. Security experts, both private and governmental, have long warned companies that data security must be a top priority. The FTC, for example, has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[9] According to the FTC, data

[7] https://web.archive.org/web/20231109192312/https://incident.mrcooperinfo.com/ (emphasis omitted).
[8] https://incident.mrcooperinfo.com/ (accessed November 13, 2023).
[9] Federal Trade Comm'n, *Start with Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

security requires: (1) encrypting information stored on computer networks; (2) retaining payment information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[10]

31. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

32. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20,

[10] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all proceeded Defendant's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

33. Although Defendant's businesses involve handling highly sensitive data, Defendant implemented inadequate data security practices that it knew or should have known, especially as a sophisticated company handling massive amounts of PII, put its customers at risk of having their sensitive data exposed.

D. The Data Breach was a Foreseeable Risk of which Defendant was on Notice

34. It is well known that PII is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect and handle such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

35. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

36. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are

not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[11]

37. Data Breach victims suffer long-term consequences when their PII, such as their Social Security numbers, are stolen and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot easily obtain new numbers.

38. Moreover, the Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[12]

39. Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet and because Defendant maintained and stored highly sensitive information that can be misused by cybercriminals and sold on the dark web.

40. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly

[11] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed March 3, 2023).
[12] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 3, 2023).

visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[13]

41. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[14]

42. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[15]

43. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[16]

44. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals

---

[13] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Feb. 24, 2023).

[14] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Feb. 24, 2023).

[15] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Feb. 24, 2023).

[16] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed March 3, 2023).

grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[17]

45. This readily available and accessible information, in addition with the widespread scope and large number of well-publicized data breach of financial institutions like Defendant, confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

46. In light of high-profile data breaches at other companies, Defendant knew or should have known that its computer systems would be targeted by cybercriminals.

47. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

48. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [18] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't

[17] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed March 3, 2023).
[18] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed March 3, 2023).

guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[19]

49. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties (and professed capabilities) to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

E. At All Relevant Times Defendant Had a Duty to Properly Secure PII

50. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Defendant became aware that their PII was compromised.

51. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

52. Security standards commonly accepted among businesses that store PII accessible to the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

[19] *Id.*

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

53. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

54. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

F. Sensitive Personal Information Is Highly Valuable

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id*.

55. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[22]

56. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[23]

57. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

58. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 3, 2023).

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed March 3, 2023).

[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 3, 2023).

59. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

60. This data, as one would expect, demands an extremely high price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

61. SPI can be used to distinguish, identify, or trace an individual's identity. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[27]

62. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

63. Much of the PII believed to be compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

---

[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed March 3, 2023).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed March 3, 2023).

[27] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed March 3, 2023).

64. Although Defendant recognizes the risk of the victims of its Data Breach, Defendant has offered no remedial measures to Plaintiff or Class Members to protect their PII and credit going forward. In fact, Defendant puts the onus on Class Members to seek out credit reports, or place fraud alerts or credit freezes, telling customers that "**[y]ou** should immediately report any unusual activity," "**[y]ou** can also contact the three major credit bureaus," and "**you** should update your passwords frequently."[28] To date, Defendant has not offered credit monitoring to Plaintiff and the Class Members, instead offering a vague promise that it will do so in the coming weeks.[29] Plaintiff and the Class Members should not need to wait an untold number of weeks, while their PII is already on the dark web, to receive credit monitoring.

65. Defendant's "remedial" advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class Members to protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

66. These extremely limited remedial measures—or advice for Plaintiff to himself take remedial measure—are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

---

[28] *See* https://incident.mrcooperinfo.com/ (emphasis added) (last accessed November 13, 2023).
[29] *Id.*

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

G. Defendant Failed to Comply with FTC Guidelines

68. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[31] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

70. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts

[30] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed March 3, 2023).

[31] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed March 3, 2023).

in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[32]

71. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[33]

72. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

---

[32] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed March 3, 2023).
[33] *See* FTC, *Start With Security*, *supra*.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

73. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. Because Class Members entrusted Defendant with their PII, Defendant had, and has, a duty to the Plaintiff and Class Members to keep their PII secure.

75. Plaintiff and the other Class Members reasonably expected that when they provided PII to Defendant, directly or indirectly, Defendant would safeguard their PII.

76. Defendant was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff and members of the Class. Defendant was also aware of the significant repercussions if it failed to do so.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including, on information and belief, Plaintiff's and Class Members' first names, last names, addresses, dates of birth, Social Security numbers, and other highly sensitive and confidential information such as, potentially, banking information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

H. Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security.

78. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Plaintiff and Class Members provided to Defendant, directly or indirectly, sensitive personal information, including Plaintiff's and Class Members' names, addresses, dates of birth, Social Security numbers, and other PII.

79. Cybercriminals intentionally attack and exfiltrate PII in order to exploit it. Thus, Plaintiff and Class Members are now, and for the rest of their lives will be, at a heightened and

substantial risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of monitoring his accounts.

80. The cybercriminals who obtained the Plaintiff's and Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

81. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

82. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

83. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

84. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[34] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

85. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

I. Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft.

86. Data Breaches such as the one experienced by Plaintiff and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

87. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[35] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps Data Breach

---

[34] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed March 3, 2023).

[35] https://www.gao.gov/assets/gao-19-230.pdf (last accessed March 3, 2023).

victims (like Plaintiff and Class Members) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

88. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[36]

89. The FTC, like the GAO recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

90. Theft of Private Information is also gravely serious. PII is a valuable property right.[38]

91. It must also be noted there may be a substantial time lag — measured in years — between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

---

[36] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed March 3, 2023) ("2007 GAO Report").
[37] *See* https://www.identitytheft.gov/Steps (last accessed March 3, 2023).
[38] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("SPI") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("SPI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

92. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

93. There is a strong probability that the entirety of the stolen information has been or will be put up for sale or otherwise be made available on the dark web, meaning every Class Member, including Plaintiff, is at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

J. Plaintiff's Experience

94. Plaintiff Rey Borge is a California resident who was the authorized payor on a home loan that was serviced by Defendant. In order to obtain home loan services from Defendant, Plaintiff was required to provide his PII to Defendant, including sensitive information such as his name, address, date of birth, phone number, Social Security number, and banking information.

95. Plaintiff Borge reasonably expected that his highly personal information would remain safeguarded and would not be accessible by unauthorized parties.

96. However, on or about November 13, 2023, Plaintiff Borge learned of the Data Breach and the risk of his PII being misused by unlawful actors. Defendant has not provided Plaintiff Borge with any remedial measures.

97. Subsequent to and as a direct and proximate result of the Data Breach, Plaintiff Borge has experienced indicia of nefarious uses of his PII. Following the Data Breach, Plaintiff Borge experience a marked increase in suspicious and nefarious text messages, calls, and emails.

In many instances, these nefarious contacts sought to deceive Plaintiff Borge into transferring money out of his accounts.

98. Plaintiff Borge is very careful about sharing and protecting his PII. Plaintiff Borge has never knowingly transmitted unencrypted PII over the internet or any other unsecured channel. Plaintiff Borge conscientiously changes his passwords in order to preserve the security of his PII.

99. Plaintiff Borge suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including needing to monitor banking and other accounts to ensure his information is not being used for identity theft and fraud; (b) damages to and diminution of the value of the PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of mitigation efforts required as a result of the Data Breach.

100. In addition, knowing that hackers accessed and exfiltrated his PII and that this likely has been and will be used in the future for identity theft, fraud, and related purposes has caused Plaintiff Borge to experience significant frustration, anxiety, worry, stress, and fear. Because he is reliant on his bank account to last him through his retirement, Plaintiff Borge is especially concerned and interested on a continuing basis in his PII remaining protected and safeguarded.

101. Despite Defendant's failure to reasonably protect Plaintiff's and the Class's PII, Defendant has not offered any compensation or adequate remedy, especially considering the significant and long-term risk Plaintiff and the Class Members face.

CLASS ALLEGATIONS

102. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

All individuals whose PII was compromised due to the Data Breach.

103. Excluded from the class are Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

104. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

105. **Numerosity**. Consistent with Fed. R. Civ. P. 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff is informed and alleges that there are millions of members of the Class. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

106. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendant knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether Defendant controlled and took responsibility for protecting Plaintiffs' and the Class's data when it stored that data on its servers;

c. Whether Defendant's security measures were reasonable in light of the recommendations of the Department of Human Health and Services, the FTC data security recommendations, state laws and guidelines, and common recommendations made by data security experts;

d. Whether Defendant owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether Defendant's failure to adequately secure Plaintiffs' and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Defendant's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiffs' and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Defendant's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

107. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class are each persons whose PII was breached by an unauthorized

third party during the Data Breach. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief due to the Class.

108. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated numerous data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

109. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

110. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CLAIMS

COUNT I
Negligence

111. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

112. Defendant owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the highly sensitive data it managed and stored on behalf of its clients. This duty arises from multiple sources.

113. Defendant owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendant's data systems, software, and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Defendant alone controlled its technology, infrastructure, and cybersecurity. Defendant further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiffs and the Class. Furthermore, Defendant knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

114. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiffs' and the Class's sensitive data and is a further source of Defendant's duty to Plaintiffs and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect highly sensitive data. Defendant, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach

orders described herein further form the basis of Defendant's duties to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

115. Defendant is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

116. Defendant breached its duty to Plaintiff and the Class by implementing unreasonable data security measures and by failing to keep data security "top-of-mind" despite understanding and the risk of data breaches involving highly sensitive data and touting its own security capabilities.

117. Defendant was fully capable of preventing the Data Breach. Defendant, as a sophisticated, experienced, and massive company, knew of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited the scope and depth of the Data Breach. Defendant thus failed to take reasonable measures to secure its systems, creating vulnerability to a breach.

118. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*

119. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

120. Defendant's unreasonable data security measures and failure to timely and with meaningful information notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

121. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect sensitive data. The FTC publications and orders described above also form the basis of Defendant's duty.

122. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the highly sensitive nature and amount of data it stored on its services and the foreseeable consequences of a Data Breach should Defendant fail to secure its systems.

123. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

124. Plaintiff and the Class are within the class of persons Section 5 of the FTCA and similar state statutes were intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act and similar state statutes were intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiffs and the Class.

125. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury.

COUNT III
Declaratory and Injunctive Relief

126. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

127. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

128. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

129. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed and continues to owe a legal duty to secure the sensitive information with which it is entrusted, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

130. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its clients' (*i.e.*, Plaintiffs' and the Class's) data.

131. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

132. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

133. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

134. Wherefore, Plaintiff, on behalf of himself and the Class, request that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and his counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all claims so triable.

Respectfully submitted,

Dated: November 17, 2023

/s/Ryan L Thompson

Ryan L. Thompson, SBN 24046969
THOMPSON LAW LLP
3300 Oak Lawn Ave., 3rd Floor
Dallas, TX 75219
Telephone: (214) 755-7777
Facsimile: (214) 716-0116
rthompson@triallawyers.com

Brian C. Gudmundson*
Jason P. Johnston*
Michael J. Laird*
Charles R. Toomajian*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
charles.toomajian@zimmreed.com

Christopher D. Jennings*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Telephone: (501) 372-1300
chris@yourattorney.com

* To be admitted *pro hac vice*
Counsel for Plaintiff and the Proposed Class